Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer-implemented method for computing the number of points on an elliptic curve over a finite field, in which a Frobenius equation is solved to a given precision by first and second parts, wherein said parts comprise the following steps, the method comprising:

receiving an elliptic curve having a total number of points on the entire curve; and

determining the total number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision, wherein the solving includes:

a) computing, to the reduced precision, a first partial solution of said lifted Frobenius equation using said first part recursively,

b) a Frobenius operation to said first partial solution,

c) computing an error term for said lifted Frobenius equation,

d) computing correction factors for said lifted Frobenius equation,

e) computing, to the reduced precision, a second partial solution of a modified lifted Frobenius equation that includes the error term and the correction factors using said second part, wherein computing the second partial solution includes:

computing, to the reduced precision, a third partial solution of said modified lifted Frobenius equation using said second part recursively applying a Frobenius operation to said third partial solution,

updating said error term,

computing, to the reduced precision, a fourth partial solution of said modified lifted Frobenius equation using said second part recursively,

combining said third partial solution and said fourth partial solution to create the second partial solution,

f) combining said first partial solution and said second partial solution to provide the solution at the full precision.

2. (Previously Presented) The method of claim 1 in which said reduced precision is one half of said full precision.

3. (Original) The method of claim 1 in which said first and second parts compute the Teichmüller lift of a given finite-field polynomial.

4. (Original) The method of claim 1 in which said first and second parts compute the canonical lift of said elliptic curve.

5. (Original) The method of claim 1 in which said first and second parts compute the multiplicative representative of a given finite-field element.

6. (Original) The method of claim 1 in which said first and second parts compute the trace of a given p-adic number.

7. (Original) The method of claim 1 in which said first and second parts compute the norm of a given p-adic number.

8. (Currently Amended) The method of claim 10, further comprising:

receiving a sequence of elliptic curves and determining the total number of points on each elliptic curve, in which said first and second parts analyze the sequence of elliptic curves.

9. (Previously Presented) The method of claim 8, further comprising:

generating a cryptographic key for use in a digital processing system using one of the secure elliptic curves.

10. (Currently Amended) The method of claim 1, further comprising:

based on the total number of points, identifying whether the elliptic curve is a secure elliptic curve for generating a cryptographic key.

11. (Currently Amended) The method of claim 1, further comprising:

storing the total number of points on the elliptic curve in a memory of the computer.

12. (Currently Amended) A computer readable medium embodying program code for directing one or more processors to perform an operation for computing the number of points on an elliptic curve, the operation comprising the steps of:

receiving an elliptic curve having a total number of points on the entire curve; and

determining ~~a~~ the total number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision, wherein the solving includes:

a) computing, to the reduced precision, a first partial solution of said lifted Frobenius equation using said first part recursively,

b) applying a Frobenius operation to said first partial solution,

c) computing an error term for said lifted Frobenius equation,

d) computing correction factors for said lifted Frobenius equation,

e) computing, to the reduced precision, a second partial solution of a modified lifted Frobenius equation that includes the error term and the correction factors using said second part, wherein computing the second partial solution includes:

computing, to the reduced precision, a third partial solution of said modified lifted Frobenius equation using said second part recursively,

applying a Frobenius operation to said third partial solution,

updating said error term,

computing, to the reduced precision, a fourth partial solution of said modified lifted Frobenius equation using said second part recursively,

combining said third partial solution and said fourth partial solution to create the second partial solution,

f) combining said first partial solution and said second partial solution to provide the solution at the full precision.

13. (Currently Amended) The computer readable medium of claim 12, wherein the operation further comprises the step of:

based on the total number of points, identifying whether the elliptic curve is a secure elliptic curve for generating a cryptographic key.

14. (Currently Amended) A integrated circuit configured to compute the number of points on an elliptic curve, the integrated circuit comprising:

logic that receives an elliptic curve having a total number of points on the entire curve;

logic that determines ~~a~~ the total number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision, wherein the solving includes:

a) computing, to the reduced precision, a first partial solution of said lifted Frobenius equation using said first part recursively,

b) applying a Frobenius operation to said first partial solution,

c) computing an error term for said lifted Frobenius equation,

d) computing correction factors for said lifted Frobenius equation,

e) computing, to the reduced precision, a second partial solution of a modified lifted Frobenius equation that includes the error term and the correction factors using said second part, wherein computing the second partial solution includes:

computing, to the reduced precision, a third partial solution of said modified lifted Frobenius equation using said second part recursively,

applying a Frobenius operation to said third partial solution,

updating said error term,

computing, to the reduced precision, a fourth partial solution of said modified lifted Frobenius equation using said second part recursively,

combining said third partial solution and said fourth partial solution to create the second partial solution,

f) combining said first partial solution and said second partial solution to provide the solution at the full precision.

15. (Currently Amended) The integrated circuit of claim 14, further comprising:

logic for identifying, based on the total number of points, the elliptic curve as a secure elliptic curve for generating a cryptographic key.